IN THE CLAIMS

Please amend the claims as follows:

Claims 1-15 (Canceled).

Claim 16 (Currently Amended): A denial-of-service attack detecting system for detecting a denial-of-service attack on a communication device, the denial-of-service attack detecting system comprising:

a monitoring device that monitors each packet transmitted to the communication device and includes a traffic abnormality detecting unit that detects traffic abnormality information indicating an abnormality of traffic based on packets transmitted to the communication device;

a performance measuring device that measures response performance of the communication device ~~by sending~~ based on a performance abnormality detection condition including a response time from transmission of a response request message to the communication device, to reception of a response message corresponding to the response request message, the performance measuring device being ~~and is~~ separate from the communication device and the monitoring device, the performance measuring device including a performance abnormality detecting unit that detects performance abnormality information indicating an abnormality of throughput of the communication device; and

an attack determining device that is connected to and performs communication with the monitoring device and the performance measuring device,

the attack determining device including an effects determining unit that determines whether the communication device has received the denial-of-service attack, using both the traffic abnormality information and the performance abnormality information, and

the effects determining unit determining that the communication device has received the denial-of-service attack, when it is determined that one of the traffic abnormality information and the performance abnormality information causes an occurrence of one of the traffic abnormality information and the performance abnormality information based on an abnormality occurrence time included in the traffic abnormality information and the performance abnormality information.

Claim 17 (Previously Presented): The denial-of-service attack detecting system according to claim 16, wherein

the monitoring device further includes a traffic-abnormality-information transmitting unit that transmits the traffic abnormality information to the attack determining device.

Claim 18 (Previously Presented): The denial-of-service attack detecting system according to claim 16, wherein

the performance measuring device further includes a performance-abnormality-information transmitting unit that transmits the performance abnormality information to the attack determining device.

Claim 19 (Previously Presented): The denial-of-service attack detecting system according to claim 16, wherein

the traffic abnormality detecting unit detects the traffic abnormality information based on a predetermined attack detection condition that is set in advance.

Claim 20 (Previously Presented): The denial-of-service attack detecting system according to claim 19, wherein

the monitoring unit further includes a signature generating unit that generates a signature indicating a feature of a packet attacking the communication device, based on the attack detection condition, and

the traffic abnormality information includes the signature.

Claim 21 (Previously Presented): The denial-of-service attack detecting system according to claim 16, wherein

the traffic abnormality detecting unit detects the traffic abnormality information based on a steady traffic indicating an average traffic of packets transmitted to the communication device.

Claim 22 (Previously Presented): The denial-of-service attack detecting system according to claim 16, wherein

the performance abnormality detecting unit detects the performance abnormality information based on a predetermined performance abnormality detection condition that is set in advance.

Claim 23 (Previously Presented): The denial-of-service attack detecting system according to claim 22, wherein

the performance abnormality detection condition includes

a response time from transmission of the response request message to the communication device to reception of a response message corresponding to the response request message, and

number of times that the response time exceeds a predetermined threshold.

Claim 24 (Previously Presented): The denial-of-service attack detecting system according to claim 16, wherein

the performance abnormality detecting unit detects the performance abnormality information based on a steady response performance indicating an average response performance feature of the communication device.

Claim 25 (Cancelled).

Claim 26 (Previously Presented): The denial-of-service attack detecting system according to claim 16, wherein

when the effects determining unit determines that the communication device has received the denial-of-service attack, the attack determining device transmits the traffic abnormality information and the performance abnormality information used for the determination to a device for reporting to an operator.

Claim 27 (Previously Presented): The denial-of-service attack detecting system according to claim 16, wherein

each of the traffic abnormality information and the performance abnormality information includes a certificate, and

the effects determining unit determines whether the communication device received the denial-of-service attack, after performing an authorization based on certificates.

Claim 28 (Currently Amended): A method of detecting a denial-of-service attack on a communication device by using a monitoring device that monitors each packet transmitted to the communication device, a performance measuring device that measures response

performance of the communication device ~~by sending~~ based on a performance abnormality detection condition including a response time from transmission of a response request message to the communication device, to reception of a response message corresponding to the response request message, ~~and~~ the performance measuring device being [[is]] separate from the communication device and the monitoring device, and an attack determining device that is connected to and performs communication with the monitoring device and the performance measuring device, the method comprising:

detecting a traffic abnormality using the monitoring device to detect traffic abnormality information indicating an abnormality of traffic based on packets transmitted to the communication device;

detecting performance abnormality information using the performance measuring device to detect performance abnormality information indicating an abnormality of throughput of the communication device; and

determining effects using the attack determining device to determine whether the communication device has received the denial-of-service attack, using both the traffic abnormality information and the performance abnormality information, the determining including determining that the communication device has received the denial-of-service attack, when it is determined that one of the traffic abnormality information and the performance abnormality information causes an occurrence of one of the traffic abnormality information and the performance abnormality information based on an abnormality occurrence time included in the traffic abnormality information and the performance abnormality information.

Claim 29 (Previously Presented): The method according to claim 28, further comprising:

transmitting traffic abnormality information using the monitoring device to transmit the traffic abnormality information to the attack determining device.

Claim 30 (Previously Presented): The method according to claim 28, further comprising:

transmitting performance abnormality information using the performance measuring device to transmit the performance abnormality information to the attack determining device.